

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
4 Persons, 5 Premises, and 2 Vehicles

Case No. MJ24-025

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

4 Persons, 5 Premises, and 2 Vehicles as described in Attachment A, incorporated herein by reference

located in the \_\_\_\_\_ Western \_\_\_\_\_ District of \_\_\_\_\_ Washington \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:


Code Section	Offense Description
21 U.S.C. §§ 841, 846	distribution, possession with intent to distribute; conspiracy
18 U.S.C. § 924(c)	possession of a firearm in furtherance of a drug trafficking crime
18 U.S.C. §§ 1956, 1957	money laundering

The application is based on these facts:

- ☒ See Affidavit of Evan Leyva, continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

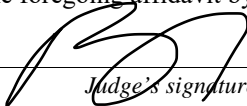
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

  
Applicant's signature

Evan Leyva, Special Agent  
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 01/19/2024

  
Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, United States Magistrate Judge  
Printed name and title

## Attachment A

## Persons, vehicles, and premises to be searched:

- a. The person of Mario James EARL (hereafter, “EARL”), born in 1978;
- b. The person of Elisa JOHNSON (hereafter, “JOHNSON”), born in 1990;
- c. The person of Maurice LYNCH (hereafter, “M. LYNCH”), born in 1975;
- d. The person of Turomne WASHINGTON (hereafter, “WASHINGTON”), born in 1989;
- e. 11527 113th PL NE, Kirkland, Washington (hereafter, “Target Premise #1”) is described as an approximately 0.1984 acre lot containing an approximately 1,380 sq ft, single-family home that is brown in color with the number 11527 clearly displayed over the garage door;
- f. 5416 Rainier Ave S, Seattle, Washington, 98118 (hereafter, “Target Premise #2”) is described as a single office space on the top floor and the furthest most right door of a multi-floor business building that sits on an approximately 0.1127 acre lot;
- g. A white Cadillac Escalade, bearing Washington state license plate CGG6626 (hereafter, the “White Escalade”);
- h. A 2021 white Tesla, WIN: 5YJSA1E64MF44189, bearing Washington license plate CFC9473 (hereafter, the “White Tesla”);
- i. 2016 S. 104th Street, Burien, Washington (hereafter, “Target Premise #3”) is described as the upstairs unit of a two-story multi-family building. The target unit has a blue front door with a poster that states “BLACK LIVES MATTER” affixed to the front door. The building has the unit number “2016” on the outside of the front of the unit;

1       j.       802 S. 31st St, Renton, Washington (hereafter, “Target Premise #4”) is  
2 described as an approximately 7,800 sq ft lot containing an approximately 2400 sq ft, 4  
3 bedroom, 2.75 bathroom, single-family home that is gray in color with the number “802”  
4 clearly displayed to the left of the garage door; and,

5       k.       1838 E 34th Street, Tacoma, Washington (hereafter, “Target Premise #5”) is  
6 described as an approximately 9,750 sq ft lot containing an approximately 1,238 sq ft,  
7 3 bedroom, and 1 bathroom, single-family home that is white with a white front door and  
8 four windows on the front side of the house.

**ATTACHMENT B**

The following items to be seized that constitute evidence, instrumentalities, or fruits of violations of Title 21 U.S.C. §§ 841 and 846 (distribution, possession with intent to distribute, and conspiracy to distribute and to possess with intent to distribute controlled substances) as well as the related offenses under Title 18 U.S.C. § 924(c) (possession of a firearm in furtherance of a drug trafficking crime) and §§ 1956 and 1957 (money laundering) are as follows:

- a. Controlled substances, including cocaine
- b. Documents reflecting the purchase or sale of controlled substances, such as ledgers, customer lists, supplier lists, correspondence, contracts and agreements between buyers and sellers, notations, logs, receipts, journals, books and/or other papers noting the price, quantity or quality of controlled substances, or noting the person or location to or from whom controlled substances were obtained, transferred, sold or distributed and/or indicating amounts due or owed on account or transactions, and any other form of ledger recordation, or papers relating to drug trafficking or money laundering during the period of January 1, 2018 to the present;
- c. Financial records reflecting illicitly obtained monies and/or other forms of assets acquired through the sales, trafficking, or distribution of controlled substances from January 1, 2018 to the present, which include federal and state tax returns, employment papers, banking records and pass books, account information, canceled checks, deposit records, income and expenditures records, property acquisition records, money market accounts and/or similar accounts, records of stocks and/or bonds purchased or exchanged; credit card records; records reflecting the rental of safe deposit boxes; safe deposit box keys; records reflecting vehicles owned, purchased, sold or leased; insurance documents; and any other documents recording or relating to the acquisition, conversion, movement, secreting, transfer and disbursement of currency and currency equivalents, including any records identifying the source or receipt and disposition of such funds, such as Currency Transaction Reports (CTRs) and Forms 8300;
- d. United States Currency, foreign currency, and financial instruments, including but not limited storage devices, keys and seed phrases utilized to store, secure, and or recreate digital currency and or wallets;

- e. Any and all business or financial records of businesses under the MCM Realty, LLC name or used to promote MCM Realty LLC;
- f. Any and all documents referring or relating to the purchase or sale of real estate properties during the period of January 1, 2016, to the present, including but not limited to purchase or sale agreements or offers; applications for property loans; property loan documents; escrow documents and payment coupons, books, or receipts; property tax documents; canceled checks or cashier check copies or receipts reflecting payment of loans or property tax bills;
- g. Any and documents relating to the rental of properties, including lease agreements and applications;
- h. Articles of personal property and documents tending to show payment, receipt, concealment, transfer, disposition of or movement of large amounts of money during the period of January 1, 2018, to the present, including bank account records; bank statements; safe deposit box keys or records; money containers; financial records or notes; ledger books; stock certificates; certificates of deposit, bonds or other financial instruments; vehicles; precious metals or jewelry; electronic equipment; or any wire transfer records, negotiated or unnegotiated checks, check stubs or receipts, traveler's checks, money orders, cashier's checks reflecting transactions involving \$1,000 or more;
- i. Money counting machines, money wrappers, vacuum sealers and bags, work sheets, tally-sheets and ledger sheets reflecting or accounting for monies and/or controlled substances received, disbursed or exchanged, and to include monies obtained from the sale and/or trafficking of controlled substances; and other equipment and materials used for processing and storing drug proceeds or U.S. currency;
- j. Records, generated during the period of January 1, 2018, to the present, of off-site locations to store records, including safe deposit box keys, records and receipts and rental agreements for storage facilities;
- k. Records regarding notes payable and receivable, IOUs, and evidence of debts owed from the time period of January 1, 2018, to the present;
- l. Photographs or videos of conspirators, controlled substances, or of assets, including U.S. currency;
- m. Records, items and documents, from January 1, 2018, to the present, reflecting travel including but not limited to passports, airline tickets, receipts, or emails notating travel, vehicle rental receipts, credit card receipts, gas station receipts,

1 and restaurant receipts, canceled checks, maps and records of long-distance calls  
2 reflecting domestic and foreign travel;

3 n. Any and all correspondence, work papers and notes related to the drug conspiracy;

4 o. Security cameras, recordings therefrom, and items use with the security system,  
5 such as televisions;

6 p. Electronic devices and storage media including laptop and desktop computers,  
7 cellular phones, tablet computers, hard drives, thumb drives, CDs, and DVDs  
8 (collectively, "electronic devices"), including Subscriber Identity Module ("SIM")  
cards and chargers associated with the devices, and the contents thereof, including:

9 i. Any and all stored communications, including, but not limited to voice  
10 calls, text messages, stored voice mail or other audio messages, recordings  
11 of incoming and outgoing calls, emails, all of which are stored or saved in  
12 the electronic devices and/or the SIM card associated with said electronic  
13 devices, that evidence the transportation, ordering, distribution, possession  
and sale of controlled substances, the collection of drug proceeds, and/or  
the connection to known and as yet unidentified co-conspirators;

14 ii. Photographs and videos that show the transportation, ordering, distribution,  
15 possession and sale of controlled substances, the collection of drug  
16 proceeds, and/or the connection to known and as yet unidentified co-  
conspirators;

17 iii. Calendar information, note pad, and other notes/records that evidence the  
18 transportation, ordering, distribution, possession and sale of controlled  
19 substances, the collection of drug proceeds, and/or the connection to known  
and as yet unidentified co-conspirators;

- iv. Phone directory, contacts, address and/or telephone books, and other records reflecting names, addresses (including email), telephone numbers, and/or the connection to known and as yet unidentified co-conspirators:
- v. Evidence of user attribution showing who used or owned the electronic devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history:
- vi. Location information that may show travel history and locations used to facilitate drug trafficking and money laundering
- q. Addresses and/or telephone books, rolodex indices and any papers or electronically stored data reflecting names, addresses, telephone numbers, pager numbers, fax numbers and/or telex numbers of co-conspirators, sources of supply, and/or customers;
- r. Indicia, both digital and otherwise, of occupancy, residency, rental and/or ownership of the property, and other properties or assets, including, but not limited to, utility, telephone, cable, and other service provider bills, insurance records, cancelled checks, receipts, rental, purchase or lease agreements, and keys;
- s. Any and all secured and/or locked rooms, hidden rooms, safes, cabinets, boxes, etc. wherein documents and currency may be located;
- t. Financial statements/records, loan records, payment journals, signature cards, keys and/or other items/records identifying assets or evidencing legitimate income (or the lack thereof); general living expenses; the obtaining, secreting, transferring, and/or concealing of assets; and the obtaining secreting, transferring, concealing, and/or spending of money.
- u. Jewelry

As used above, the terms records, documents, programs, applications, or materials includes records, documents, programs, applications, or materials created, modified, or stored in any form.

During the execution of the search of the Subject Persons, Vehicles, or Premises described in Attachment A, if law enforcement encounters a smartphone or other

1 | electronic device equipped with a biometric-unlock feature, and if law enforcement  
2 | reasonably suspects Mario James EARL, Elisa JOHNSON, Maurice LYNCH, and/or  
3 | Turomne WASHINGTON is a user of the device, then – for the purpose of attempting to  
4 | unlock the device in order to search the contents as authorized by this warrant – law  
5 | enforcement personnel are authorized to: (1) press or swipe the fingers (including  
6 | thumbs) of the individuals to the fingerprint scanner of the device; and/or (2) hold the  
7 | device in front of the face and open eyes of those same individuals and activate the facial,  
8 | iris, or retina recognition feature.

9 |         In pressing or swiping an individual’s thumb or finger onto a device and in  
10 | holding a device in front of an individual’s face and open eyes, law enforcement may not  
11 | use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically,  
12 | law enforcement may use no more than objectively reasonable force in light of the facts  
13 | and circumstances confronting them.



STATE OF WASHINGTON           )  
  )           SS  
COUNTY OF KING             )

## AFFIANT BACKGROUND

2. I am a Special Agent with the DEA and have been so employed since March 2020. As a DEA Special Agent, I have received approximately four months of specialized training at the DEA Training Academy in Quantico, Virginia. This training focused on methods of unlawful drug trafficking; the means by which drug traffickers and/or manufacturers derive, launder, and conceal their profits from drug trafficking; the use of assets to facilitate unlawful drug trafficking activity; and the law permitting the forfeiture to the United States of assets purchased with drug proceeds or assets used or intended to be used to facilitate the drug violations. Since completion of the DEA Academy, I have been assigned to the DEA's Atlanta Division Office Enforcement Group One and have been so assigned since October 2020. Prior to my employment as a Special Agent with the DEA, I was employed as a Narcotics Investigator and Georgia Peace Officer with the Gwinnett County Police Department for over three years. During this time, I have arrested individuals who have been charged with trafficking, possession with intent to distribute, sale, and/or possession of illegal drugs, including marijuana. I have written and/or participated in the execution of search warrants resulting in the

1 seizure of marijuana, cocaine, methamphetamine, heroin, MDMA, prescription pills, and  
2 other illegal narcotics. These search warrants have also resulted in the seizure of U.S.  
3 currency, ledger books, drug customer information lists, bank statements, packaging  
4 materials, cellular phones, and other items related to the possession, sale, and distribution  
5 of illegal narcotics and money laundering. I have also attended formal and informal  
6 narcotics related training through the Gwinnett County Police Department.

7 3. In connection with my official DEA duties, I investigate criminal violations  
8 of state and federal drug laws and related offenses, including, but not limited to,  
9 violations of Title 21, United States Code, §§ 841, 843, 846, 848, 856, 952, 960, and 963,  
10 and Title 18, United States Code, §§ 1956 and 1957.

11 **INTRODUCTION AND PURPOSE OF AFFIDAVIT**

12 4. This affidavit is submitted for the limited purpose of establishing probable  
13 cause to search the locations listed below, more particularly described in Attachment A  
14 hereto (collectively, the “**Target Premises**”), for evidence of persons known and  
15 unknown, who have committed, are committing, and will continue to commit federal  
16 felony offenses, and evidence of the commission of those offenses, to wit, possession of  
17 controlled substances with intent to distribute in violation of Title 21, United States Code,  
18 Section 841(a)(1); attempt and conspiracy to commit an offense in violation of Title 21,  
19 United States Code, Section 846; money laundering in violation of Title 18, United States  
20 Code, Sections 1956; attempt and conspiracy to commit money laundering in violation of  
21 Title 18, United States Code, Section 1956 and aiding and abetting the same in violation  
22 of Title 18, United States Code, Section 2 (“**Target Offenses**”), all as described in  
23 Attachment B: hereto:

- 24 a. The person of Mario James EARL (hereafter, “EARL”), born in 1978.  
25 b. The person of Elisa JOHNSON (hereafter, “JOHNSON”), born in 1990.  
26 c. The person of Maurice LYNCH (hereafter, “M. LYNCH”), born in 1975.  
27

- d. The person of Turomne WASHINGTON (hereafter, "WASHINGTON"), born in 1989.
- e. 11527 113th PL NE, Kirkland, Washington (hereafter, "Target Premise #1") is described as an approximately 0.1984 acre lot containing an approximately 1,380 sq ft, single-family home that is brown in color with the number 11527 clearly displayed over the garage door;
- f. 5416 Rainier Ave S, Seattle, Washington 98118 (hereafter, "Target Premise #2") is described as a single office space on the top floor and the furthest right door of a multi-floor business building that sits on an approximately 0.1127 acre lot;
- g. A white Cadillac Escalade, bearing Washington license plate CGG6626 (hereafter, the "White Escalade");
- h. A 2021 white Tesla, WIN: 5YJSA1E64MF44189, bearing Washington license plate CFC9473 (hereafter, the "White Tesla").
- i. 2016 S. 104th Street, Burien, Washington (hereafter, "Target Premise #3") is described as the upstairs unit of a two-story multi-family building. The target unit has a blue front door with a poster that states "BLACK LIVES MATTER" affixed to the front door. The building has the unit number "2016" on the outside of the front of the unit.
- j. 802 S. 31<sup>st</sup> St, Renton, Washington (hereafter, "Target Premise #4") is described as an approximately 7,800 sq ft lot containing an approximately 2400 sq ft, 4 bedroom, 2.75 bathroom, single-family home that is gray in color with the number "802" clear displayed to the left of the garage door.
- k. 1838 E 34th Street, Tacoma, Washington (hereafter, "Target Premise #5") is described as an approximately 9,750 sq ft lot containing an approximately 1,238 sq ft, 3 bedroom, and 1 bathroom, single-family home that is white, with a white front door, and four windows on the front side of the house.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. I have not included every fact concerning this investigation. Rather, I have set forth the facts that I believe are necessary for a fair determination of probable cause. Based on the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that the

1 items described in Attachment B will be found at the locations described in Attachment  
2 A, and constitute evidence, fruits, and instrumentalities of violations of Title 21 U.S.C.  
3 Sections 841, 846, and 856, and Title 18 U.S.C. Section 1956.

4 **SUMMARY OF PROBABLE CAUSE**

5 6. Since December 2021, DEA Atlanta has been investigating a Drug  
6 Trafficking and Money Laundering Organization lead by Mario EARL (hereafter referred  
7 to as the EARL DTO or the DTO) which is responsible for distributing thousands of  
8 kilograms of cocaine throughout the United States, on a yearly basis. Agents learned that  
9 the DTO would receive kilogram quantities of cocaine shipments which they would store  
10 at DTO stash houses.<sup>1</sup> The DTO would then sell kilogram quantities of cocaine to local  
11 distributors, and collect the proceeds which would be stored at the DTO stash houses.  
12 Stash house operators would record sales, proceeds received, and debts owed by buyers  
13 in both electronic and paper ledgers.

14 7. When EARL announced a money pick up, the stash house operators would  
15 compile the proceeds which would later be transported by DTO members via automobile  
16 to a different DTO stash location for a final count. Agents learned that the automobiles  
17 were equipped with traps (aftermarket hidden compartments)<sup>2</sup> and were frequently  
18 registered in the name of a DTO member, or one of their associates. In some instances,  
19 female members of the DTO would rent automobiles for male DTO members to use in  
20 furtherance of the DTO.

21 8. The investigation by DEA Atlanta between December 2021 and December  
22 of 2023, led to the identification of and search warrant executions at multiple DTO stash  
23 houses. Evidence seized from those stash houses revealed planning and coordination  
24

25 <sup>1</sup> A stash house is a location used to store illegal drugs, drug proceeds, and tools and implements of drug trafficking  
26 and money laundering. In this organization, DTO stash houses were also typically owned by a DTO member or  
associate, or rented in the name of a DTO member who did not live at the location.

27 <sup>2</sup> Based on my knowledge, training, and experience, vehicles containing traps are used to evade law  
enforcement detection while transporting large amounts of illegal narcotics, proceeds from the sale of  
illegal narcotics, and firearms used in furtherance of narcotics trafficking.

1 between DTO members, electronic and handwritten drug and money ledgers, and  
2 correspondence between members and associates of the DTO, revealing an extremely  
3 sophisticated organization operating throughout the United States.

4 **July 7, 2022, Home Invasion, and Armed Robbery, in Bergen County, NJ**

5 9. During this investigation, Agents learned that on July 7, 2022, a home  
6 invasion and armed robbery occurred at a DTO stash house used to store drugs and drug  
7 proceeds in Bergen County, New Jersey. The house was rented in the name of two DTO  
8 members: Dominique GWINN and Elisa JOHNSON.<sup>3</sup> A search of the residence revealed  
9 two large industrial size safes, one of which contained three, one-kilogram packages of a  
10 white powdery substance, which based on my knowledge, training, and experience I  
11 believe to be consistent with cocaine, a schedule II-controlled substance. The substance  
12 has been submitted for testing, but the results have not yet been received by DEA  
13 Atlanta. Also recovered from the residence was one handgun, multiple vacuum sealers,  
14 dozens of vacuum sealer bags, and numerous documents and affects bearing the names of  
15 and belonging to DTO members EARL, JOHNSON, GWINN, and Turomne  
16 WASHINGTON.

17 10. A Starbucks cup bearing the name “Mario” on the printed label was found  
18 in one of the bedrooms of the stash house. The coffee was purchased from a nearby  
19 Starbucks via EARL’s Starbucks Mobile app on the same day as the robbery. A review of  
20 surveillance footage from the Starbucks verified that EARL purchased the coffee earlier  
21 that morning. In the same bedroom, law enforcement located a bag with the embroidered  
22 initials “MJE,” (Mario James Earl) which contained medication prescribed to EARL.  
23 Law enforcement also observed utility bills and other mail that indicated the DTO had  
24 other stash locations in the New Jersey area. Laptops, four cellphones, other electronic  
25  
26  
27

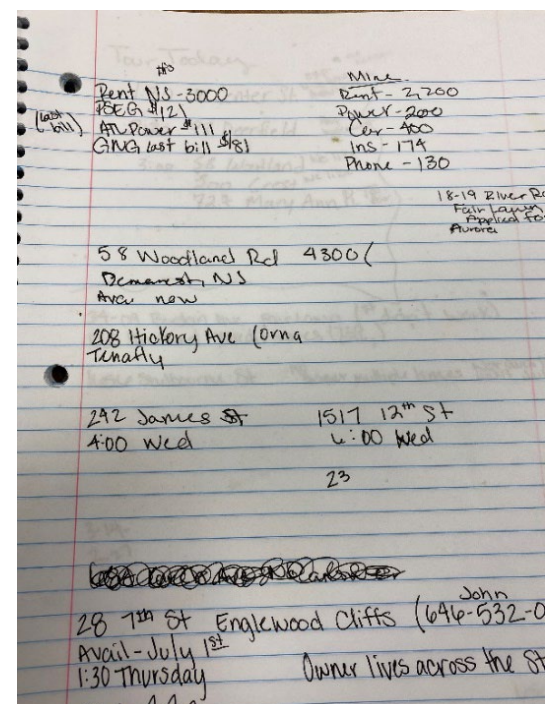
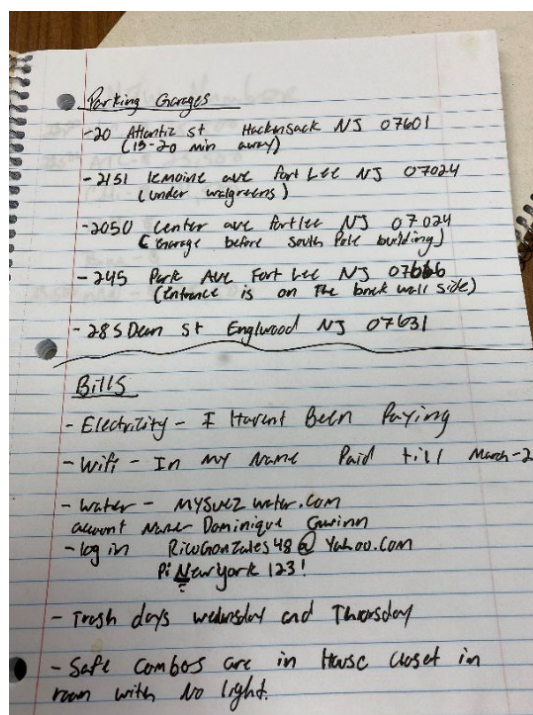
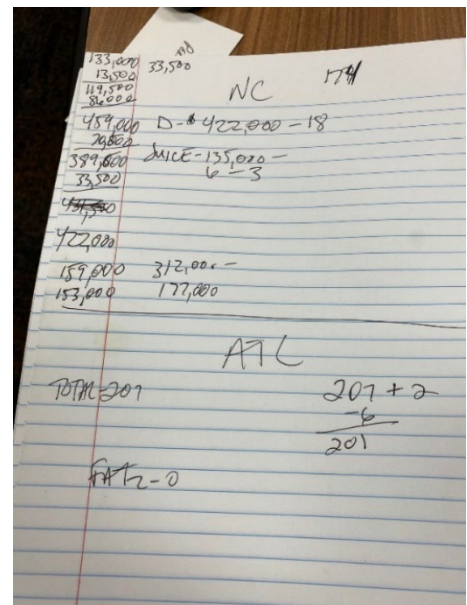
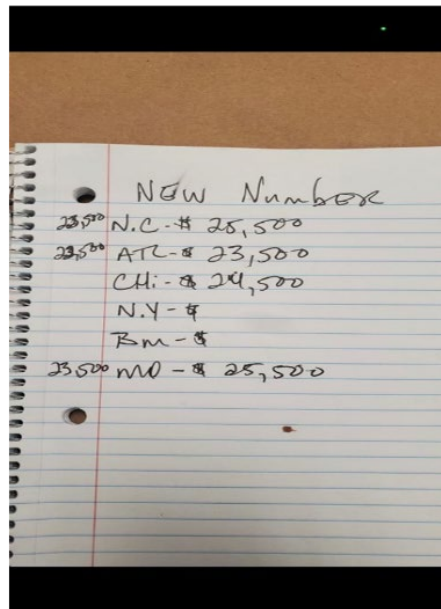
---

<sup>3</sup> Neither GWINN nor JOHNSON was present during the robbery, nor were they living in the location at any point.



storage devices, and hand-written detailed drug and money ledgers were also located inside of the residence.

11. The ledgers documented transactions, addresses of parking garages where the DTO leadership was comfortable conducting these transactions and or money pickups, bills and even the current price of cocaine per kilogram in different parts of the country, as seen in the photographs below.



1           12. An analysis of the electronic devices seized at the residence, which are  
2 believed to belong to EARL, revealed extensive communications between DTO  
3 members, as well as drug and money ledgers which detailed inventory, and money  
4 collected by several of the organization's stash houses.

5           13. One of the laptops located during the search is believed to belong to EARL.  
6 The laptop was located in close proximity to other electronic storage devices, and hand-  
7 written detailed drug and money ledgers. Law enforcement attempted to search the  
8 contents of the laptop, but were unable to due to a sophisticated password and encryption.  
9 Based on my training and experience, I believe EARL utilized that laptop to further  
10 communicate, document, and facilitate in the further distribution of cocaine and  
11 operations of the DTO.

12           14. This belief was confirmed later in the investigation when agents located  
13 email communication between EARL and other members of the DTO. These email  
14 communications consisted of instructions to rent additional stash houses as well as emails  
15 discussions about the fraudulent documents that EARL would later email to members of  
16 the DTO as proof of employment to rent said stash houses.

17           15. Based on a review of the ledgers, agents discerned that the DTO provided a  
18 regular customer with approximately 409 kilograms of cocaine from February 11, 2022,  
19 through May 7, 2022. At the start of the ledger, the customer already amassed a debt of  
20 \$648,000. The ledger also indicates that between February 11, 2022, through May 7,  
21 2022, the customer paid the DTO a total of \$8,490,615 for cocaine that was issued on  
22 credit. As of the final ledger entry, the customer still owed an outstanding debt of  
23 approximately \$782,385 to the DTO.

24           16. During the execution of the same search warrant, a Nissan Sentra registered  
25 to GWINN (which contained a trap compartment) was recovered from the driveway of  
26 the residence. Inside the residence, investigators recovered oil change paperwork for a  
27 different Nissan Sentra, bearing the name of Jovan, an address of 17336 Park Ave,

1 | Lansing, IL, 60438, and a contact number of 773-410-8857. AT&T records revealed 773-  
2 | 410-8857 to have been registered to Jovan JACKSON Sr (a high-ranking member of the  
3 | DTO) since December 30, 2020.

4 | **July 18, 2022, Search Warrant in Fairburn, GA**

5 | 17. On July 18, 2022, law enforcement was surveilling a DTO stash house in  
6 | Fairburn, GA when Maurice LYNCH (brother of high ranking DTO member Ramondo  
7 | LYNCH) exited the stash house with several bags, and entered an Uber with his teenage  
8 | daughter. During a traffic stop, M. LYNCH fled from the vehicle on foot and was  
9 | arrested after discarding a bag containing two kilograms of cocaine. A search warrant  
10 | executed at the Fairburn Stash house led to the recovery of approximately 15 kilograms  
11 | of psychedelic mushroom bars, 5 pounds of THC edibles, 2 firearms, approximately 6  
12 | cell phones, handwritten detailed drug and money ledgers, and \$112,000. Inside the  
13 | residence, Agents located documents (including money orders, bills, and receipts) which  
14 | linked EARL, R. LYNCH, M. LYNCH, and JOHNSON to the home, and led agents to  
15 | identify other DTO stash houses in the Atlanta, Georgia area, and around the country.<sup>4</sup>  
16 | Agents located flight luggage tags for Delta flights taken by EARL and JOHNSON, as  
17 | well as Amazon packages addressed to EARL, and prescription medication in his name.  
18 | Information gathered during the execution of this warrant, and the investigation of the  
19 | DTO to date, led to DEA Atlanta executing an additional state search warrant in  
20 | Baltimore, MD two days later.

21 | **July 20, 2022, Search Warrant in Baltimore, MD**

22 | 18. On July 20, 2022, DEA Atlanta, in conjunction with DEA Baltimore,  
23 | executed a state search warrant at a Baltimore stash house where DTO member R.  
24 | LYNCH was being surveilled. R. LYNCH fled prior to the execution of the search  
25 |  
26 |

27 | <sup>4</sup> Agents also located numerous black dog kennels and cages in the garage of the home, some of which contained French bulldogs.



1 warrant. At the residence, agents located an additional Nissan Sentra<sup>5</sup> parked in the  
2 garage of the home. The Sentra was equipped with a trap compartment in the floorboard  
3 of the vehicle, which contained approximately \$85,000 in vacuum-sealed packaging and  
4 a stolen firearm. Agents also located approximately three cell phones, handwritten  
5 detailed drug and money ledgers, and an additional \$15,000 in U.S. Currency in the  
6 residence.

7 **GPS Ping for Phones used by JOHNSON & GWINN**

8 19. On August 16, 2022, Bergen County Prosecutors Office received search  
9 warrants for the GPS Ping monitoring of cellular devices used by JOHNSON and  
10 GWINN. Using those pings, agents were able to surveil GWINN and JOHNSON, and  
11 were able to identify numerous stash houses where the DTO stored cocaine, other illegal  
12 drugs, and drug proceeds. Through electronic and physical surveillance agents were also  
13 able to observe how the DTO transported cocaine and/or drug proceeds from one stash  
14 house to another, across state lines, between at least six different states. Eventually,  
15 agents sought and were granted warrants to search additional DTO stash houses in the  
16 states of Georgia, New York, New Jersey, and North Carolina.<sup>6</sup>

17 **September 15, 2022 - Search Warrants executed at GWINN's Apartment and**  
18 **JACKSON's Residence**

19 20. On September 15, 2022, DEA Atlanta executed warrants at an Atlanta,  
20 Georgia apartment rented by GWINN and a house owned by high-ranking DTO member  
21 Jovan JACKSON in, Snellville, GA. No evidence was recovered from GWINN's  
22 apartment, which appeared vacant. However, agents noticed several empty duffle bags  
23 inside the apartment, and seized a Nissan Sentra (registered to GWINN and affixed with  
24

---

25 <sup>5</sup> DEA Atlanta has identified multiple different Nissan Sentras used by this DTO to traffic narcotics and  
26 proceeds, all of which contain traps. Two of the DTO Nissan Sentras were registered to Dominique  
27 Gwinn.

<sup>6</sup> Although the DEA identified an additional suspected stash location in Chicago, Illinois, a search warrant was not  
executed at that location.

her parking pass) from the apartment complex parking deck. The vehicle contained an empty trap compartment. Agents are aware that GWINN was actively living and paying rent at another location, while the rent was still being paid to maintain this apartment. For that reason, agents believe the apartment was used solely as a stash location.

21. The search of JACKSON's house revealed a Nissan Sentra parked in the garage with \$710,000 hidden in a trap compartment inside the vehicle. Agents recovered six handguns from a kitchen cabinet, multiple vacuum sealers and dozens of vacuum sealer bags from the home, several duffle bags matching the same brand and dimensions found in GWINN's apartment, and numerous documents (including but not limited to internet bills, receipts, business documents, bank account statements, and documents related to additional vehicles,) bearing Jovan and Marlene JACKSON's names, indicating they were the primary residents and owners. Agents also recovered documentary evidence of other residences utilized by the DTO, an Apple laptop, approximately six cellphones, handwritten detailed drug and money ledgers, and an additional approximately \$50,000 inside of the residence.

22. An analysis of the electronic devices seized at the residence revealed extensive stored communications and ledgers, including detailed financial notations for several of the organization's stash houses. Based on the analysis of the ledgers and communications, agents believe that the DTO distributed approximately 1,140 Kilograms of cocaine (Units) and received approximately \$15,591,599.00 in proceeds between May 1, 2022, and July 30, 2022.

**September 15, 2022 - Search and Seizure Warrants executed in Bergen County, NJ**

23. On September 15, 2022, in conjunction with DEA Atlanta, Bergen County Prosecutors Office executed state search and seizure warrants at multiple (approximately three) DTO stash locations in Bergen County New Jersey. During the execution of these warrants, approximately 1.6 million in United States currency was seized. The largest concentration of bulk US currency came from inside of a trap located inside a Jeep

Cherokee, parked outside of a DTO stash house. The 2nd largest concentration of bulk US currency came from a trap inside of a Nissan Rogue which was parked outside of a DTO stash house.<sup>7</sup> Law enforcement also recovered several money counters, handwritten detailed drug and money ledgers, vacuum sealers, and other paraphernalia consistent with packaging bulk amounts of drug proceeds.

24. Turomne WASHINGTON was arrested inside of a DTO stash location at 2030 Hudson Street, Apartment 1236, in Bergen County New Jersey. Agents found his identification, bank cards, and personal items throughout the apartment. Additionally, during the execution of these warrants, law enforcement recovered a Glock handgun located inside of a trap in a Nissan Murano which was known to be operated by WASHINGTON.

25. During the search of a DTO stash house in Englewood, New Jersey, law enforcement recovered a loaded assault rifle in a hidden room built within the residence.<sup>8</sup> Law enforcement also recovered several vehicle key fobs which were definitively linked back to the trap vehicles referenced in paragraph 20 above, as well as a “trap” vehicle previously recovered from the residence located at the DTO stash location referenced in paragraph 8 above.

26. During the search warrant executions on September 15, 2022, law enforcement also recovered four cellular devices believed to be utilized by WASHINGTON. These devices were submitted to the BCPO Digital Forensics Lab for processing. WASHINGTON was arrested and charged with one count of N.J.S.A. 2C:

---

<sup>7</sup> The car keys to the Jeep Cherokee and the Nissan Rogue, were recovered from inside one of the DTO stash locations in Bergen County, New Jersey.

<sup>8</sup> EARL has a 2009 conviction for Conspiracy to Distribute Marijuana in the Western District of Washington in case number 2009-CR-00006. In that case, EARL ran a sophisticated interstate marijuana trafficking ring along with his brother and several codefendants. A search warrant executed at EARL’s home in West Seattle on January 13, 2009, revealed distribution quantities of marijuana, a magazine for an assault rifle, ammunition, fraudulent identification documents, and a secret room in the home, specially constructed to evade casual detection which was used to store marijuana.

21-25(a), Financial Facilitation of Criminal Activity (“Money Laundering”), and N.J.S.A. 2C: 36-3, Possession with Intent to Distribute Drug Paraphernalia.

**September 15, 2022 - Search Warrant executed in Charlotte, NC**

27. On September 15, 2022, DEA Charlotte, NC executed a federal search warrant at a DTO stash location in Charlotte, NC. Agents seized approximately \$175,000 in cash and eight kilograms of a substance which field tested positive for cocaine and fentanyl (both schedule-II controlled substances), from a large industrial safe located in the home. Agents confirmed that the safe was purchased through Spartan Safe Company by DTO member Jovan JACKSON on June 24, 2022. Also recovered from the residence were multiple vacuum sealers, dozens of vacuum sealer bags and hand-written detailed drug and money ledgers. Agents also seized documents bearing Jovan JACKSON’s and Turomne WASHINGTON’s names.

**March 2, 2023 – Search warrant executed at Ramondo LYNCH’s residence in Sandy Springs, GA**

28. On March 2, 2023, DEA Atlanta executed a federal search warrant at 6470 Wright Circle, Sandy Springs, GA, a home owned by DTO member Ramondo Lynch. Agents were aware that no one had been inside the home since shortly after the warrant execution on the Fairburn Stash house in July of 2022. Inside the residence, agents seized numerous handwritten drug and money ledgers, bank and utility documents listing the name Ramondo LYNCH, luxury custom jewelry receipts, a vacuum sealer, and approximately nine cell phones. Analysis of the electronic devices seized at the residence revealed extensive stored communications between DTO members and associates coordinating cocaine deals, money drop offs and pickups, and detailed ledgers, which included detailed notations for several of the organization’s stash houses. Agents also located phone bills, business fillings, vehicle information, and money orders tying other DTO members to the location.

**Financial Investigation**

29. During the investigation, agents reviewed bank statements from an account owned by EARL. Based on my knowledge, training, and experience, financial institutions (banks) have transaction reporting requirements which flag cash deposits of \$10,000 or more. These reporting requirements are intended to assist law enforcement in the identification of drug proceeds and money laundering activity. I am also aware that drug traffickers who make large cash deposits into their bank accounts, split the deposits up into multiple deposits under that \$10,000 amount to avoid the financial transaction reporting requirements of banks and other financial institutions.

30. In February of 2022, a series of cash deposits were made into EARL's Wells Fargo account via in branch deposits and ATM cash deposits. Three separate deposits of \$3,000 (for a total of \$9,000) was deposited via ATM on February 5, 2022. Three additional cash deposits of \$2,900 (for a total of \$8,700) and a single deposit for \$800 were made via ATM on February 2, 2023. On February 8, 2022, three separate deposits were made into EARL's account at a Wells Fargo Branch. The first deposit was for \$9,000 the second was for \$9,800, and the third was for \$250. Based on my knowledge, training, and experience, I believe these cash deposits were split into multiple transactions in an amount under \$10,000 to avoid the transaction reporting requirements of financial institutions, and to evade law enforcement detection.

**October 24, 2023- Federal indictment for members of the DTO**

31. On October 24, 2023, a Federal Grand Jury in the Northern District of Georgia returned an indictment charging several individuals, including EARL, R. LYNCH, JACKSON, M. LYNCH, WASHINGTON, JOHNSON, and GWINN with conspiracy to distribute a controlled substance (cocaine) in violation of Title 21, United States Code, Sections 846 and 841 (Count One), and conspiracy to launder money (Count Seven), among other charges, in Case No. 1:23-CR-335 (under seal). Following the

1 indictment, the Court issued arrest warrants for each of these individuals. None of the  
2 charged defendants have been arrested yet.

3 **Identification of 11527 113th PL NE, Kirkland, WA “Target Premise #1”**

4 32. During the investigation agents learned that on or about October 26, 2012,  
5 JOHNSON purchased 11527 113th PL NE, Kirkland, WA (**Target Premise #1**). On or  
6 about July 21, 2016, **Target Premise #1** was sold by JOHNSON to EARL. A search of  
7 law enforcement data bases indicate that EARL is still the owner of **Target Premise #1**,  
8 and per the Washington State Department of Licensing (DOL) the address on EARL’s  
9 driver’s license is **Target Premise #1**.

10 33. EARL has used and continues to use a Verizon cellular device assigned call  
11 number (206) 806-1314, subscribed in the name of Mario J Earl, since October 9, 2019.  
12 The Bergen County (NJ) Prosecutors Office (BCPO) received court authorized  
13 geolocation data for (206) 806-1314, in approximately September and October of 2022.  
14 During that time, the geolocation data indicated that (206) 806-1314 was in Seattle,  
15 Washington. DEA Seattle conducted physical surveillance of EARL which consistently  
16 put EARL in the same location as the geolocation data from (206) 806-1314. Based on  
17 that information, and the continued surveillance, agents determined that EARL was in  
18 possession of (206) 806-1314.

19 34. Agents identified that JOHNSON has used and continues to use a Verizon  
20 cellular device assigned call number (206) 507-1108, subscribed in the name of Elisa I  
21 Johnson. The subscriber information lists **Target Premise #1** as the contact address  
22 associated with the account since October 19, 2018.

23 35. On January 13, 2023, DEA Atlanta obtained a geolocation warrant for  
24 (206) 507-1108, during which time DEA Atlanta and DEA Seattle conducted physical  
25 and electronic surveillance of JOHNSON . Based on the physical surveillance which  
26 consistently put JOHNSON in the same location as geolocation data from (206) 507-  
27 1108, agents determined that she was in possession of (206) 507-1108.

36. Agents learned EARL has an active Airbnb account where **Target Premise #1** has been advertised for rent. The webpage<sup>9</sup> for **Target Premise #1** indicates **Target Premise #1** has been listed for rent for approximately 1 year, with the last review provided by a renter in August of 2023. This time frame is consistent with when EARL and JOHNSON moved out of their previous apartment and moved into **Target Premise #1** full time. Even though the Airbnb webpage for **Target Premise #1** is still active, the available dates to rent **Target Premise #1** are blacked out until June 15, 2024.

37. On December 14, 2023, DEA Atlanta obtained a geolocation search warrant for the cellular devices that are known to be used by EARL and JOHNSON.

38. A review of overnight activity for both historical location data and live geolocation data placed almost every night both cellular facilities consistently connecting to the cell sites in the area of **Target Premise #1**. A review of the geolocation data also revealed that both EARL and JOHNSON often leave **Target Premise #1** together and travel to the gym around 5:45 a.m. The geolocation data shows them both stay for a reasonable amount of time then travel back to **Target Premise #1**. This is behavior is consistent with EARL and JOHNSON going back to **Target Premise #1** to shower and change after attending the gym, further indicating that **Target Premise #1** is their primary residence.

39. On December 20, 2023, during surveillance DEA Seattle agents observed JOHNSON answer the front door of **Target Premise #1** accompanied by a small dog.

40. Based on the investigation to date, along with my training and experience, I believe EARL and JOHNSON have moved into **Target Premise #1** as their primary residence and that EARL and JOHNSON will be present inside of **Target Premise #1**, when agents execute the Search warrants.

---

<sup>9</sup> [https://www.airbnb.com/rooms/713678641359624791?adults=4&pets=1&check\\_in=2023-01-05&check\\_out=2023-01-09&source\\_impression\\_id=p3\\_1672518902\\_DcA8n6PTUSNZOviZ](https://www.airbnb.com/rooms/713678641359624791?adults=4&pets=1&check_in=2023-01-05&check_out=2023-01-09&source_impression_id=p3_1672518902_DcA8n6PTUSNZOviZ)



**Identification of 5416 Rainier Ave S, Seattle, WA 98118 “Target Premise #2”**

41. During the investigation, agents learned that EARL directed JOHNSON and GWINN to rent houses and apartments around the country to be used by the DTO as stash houses. A review of several of the lease agreements for those stash houses revealed that JOHNSON and GWINN used fraudulent pay stubs provided by EARL to show proof of income. On several of the lease agreements, JOHNSON listed MCM Realty Investments LLC, 5416 Rainier Ave S, Seattle, WA 98118 (**Target Premise #2**), (a company owned by EARL) as her employer, and “James EARL” as her supervisor. The fraudulent paystubs were made to create the appearance that JOHNSON worked at and earned a salary from MCM Realty Investments, LLC located at **Target Premise #2**. Electronically stored communications between EARL, JOHNSON, and GWINN, confirmed that the paystubs were fraudulent, and were created solely to lease the locations.

42. An open-source search of MCM Realty Investments LLC identified EARL as the owner and president of the company. EARL, through MCM Realty Investments LLC, owns a building in Seattle containing **Target Premise #2**. The building has three street addresses: 5418 Rainier Ave S, Seattle, WA (bottom floor); 5416 Rainier Ave S, Seattle, WA (top floor)( **Target Premise #2**); and 4419 S Brandon street, Seattle, WA (rear of building). The building that contains **Target Premise #2**, has at least nine exterior doors: four on the south side, one on the west side, three on the north side, and at least one on the east side.

43. The company website, <https://mcmrealtyinvestments.com/>, identifies EARL as the president and advertises retail and apartment space for rent at 4419 South Brandon Street, Seattle, Washington 98118. on the website agents identified a link for the Airbnb webpage that was previously mentioned for **Target Premise #1**.

44. A review of the geolocation data for both EARL and JOHNSON shows them leaving **Target Premise #1** and then traveling to **Target Premise #2**, where they



1 would remain throughout the work hours of the day. The data then shows them both  
2 leaving **Target Premise #2** and traveling back to **Target Premise #1**. This pattern is  
3 almost on a daily basis as it pertains to EARL, but is less consistent as it pertains to  
4 JOHNSON. Based on my training and experience I believe that **Target Premise #2** is the  
5 location of EARL and JOHNSON's offices and this is confirmed based on observations  
6 made by DEA Seattle members.

7 45. Agents have reviewed video surveillance footage of the building from mid-  
8 December to early January, 2024 via a pole camera. From this review, agents believe  
9 there are many doors on the building that only access one unit, and do not connect  
10 internally with other units. There are also at least two doors that access a basement space  
11 which includes additional internal entrances to other units.

12 46. Agents have observed EARL access many points of the building, but  
13 primarily one door on the south side: the top floor, easternmost door (**Target Premise**  
14 **#2**). Agents believe this door accesses EARL and JOHNSON's office. EARL is often  
15 there alone, and others don't go in that door without him. Agents have seen other people  
16 enter **Target Premise #2**, but not without EARL or when EARL is already inside (the  
17 exception being JOHNSON).

18 47. During the observations, EARL usually parks his Cadillac Escalade in front  
19 of the building along Rainier Ave S or on a side street next to the building. EARL usually  
20 carries a briefcase or bag with him when entering **Target Premise #2**. On an almost daily  
21 basis, agents observe EARL arrive in the morning and enter **Target Premise #2** and stay  
22 most of the day. EARL appears to unlock the door to **Target Premise #2** when he  
23 arrives, suggesting it was not open to the public or to others without him. JOHNSON was  
24 also seen using a key to access **Target Premise #2** on her own. It appears EARL is  
25 keeping regular business hours at this location, in the south side, second floor,  
26 easternmost door (**Target Premise #2**).  
27

48. A photo of the south side of **Target Premise #2** the building, with EARL's office door highlighted in yellow is depicted below:



49. Agents have also observed EARL regularly going into a door on the north side of the building, which is accessed off Brandon Street. From photos on the MCM Realty Investments website, it appears this door opens to a stairwell which accesses multiple basement level units. Agents have noticed many other people use this door, with or without EARL. Since EARL owns the building, he may be going in and out of this door for regular maintenance and there are portions of the building under construction. EARL has been seen coming and going from this door with tools and other construction equipment. Based on the presence of hidden rooms in other stash locations used by EARL in his prior case and in a DTO safe house in this case, there may be hidden rooms containing evidence of the DTO's operation on the premises.

50. During the surveillance of EARL, he has and continues to be observed driving a white Cadillac Escalade, bearing Washington license plate CFC6626 hereafter, the "**White Escalade.**" The **White Escalade** is registered to MCM Realty Investments, LLC and Mario EARL at 5418 Rainier Ave S, Seattle, WA.

51. During these observations, JOHNSON has and continues to be observed driving a white Tesla, bearing Washington license plate CGG6626 (hereafter, the "**White Tesla**"), registered to Elisa JOHNSON at 11410 NE 124 street #243, Kirkland, WA.

This address is for a UPS store P.O. box #243.

52. Based on my training and experience, and observations made by DEA Seattle, I believe that EARL and JOHNSON are using **Target Premises #2** as their office. Additionally, I believe that EARL is transporting potential evidence inside of his briefcase/bag from **Target Premises #1** to inside of **Target Premises #2**. It is common for people to use a briefcase/bag to store and or transport computers, tablets, documents, and other storage devices from one location to another.

**Identification of 2016 S 104th Street, Burien, Washington “Target Premise #3”**

53. During the investigation agents identified a JPMorgan Chase Bank account utilized by WASHINGTON, and subpoenaed bank information and records for the account. In those records WASHINGTON provided 2016 S104th Street, Burien, Washington (**Target Premises #3**) as his personal address when opening the account on July 5, 2022.

54. On September 15, 2022, WASHINGTON was arrested during the execution of a search warrant in Bergen County, New Jersey, at a known stash location utilized by the DTO. During his arrest, WASHINGTON’s cellular telephone was seized as evidence. That telephone is still in the possession of law enforcement. WASHINGTON was released on bond from the Bergen County Jail on September 26, 2022, and activated a T-Mobile cellular device assigned call number (201) 233-9590 on September 27, 2022.

55. WASHINGTON has and continued to use (201) 233-9590. Shortly after the activation of (201) 233-9590, WASHINGTON provided (201) 233-9590 to the Washington State Department of Corrections as his contact number as a requirement of his status as a registered sex offender. (201) 233-9590 was also provided as a number where WASHINGTON’s parole officer could reach him. On February 10, 2023, at his annual check in with parole, WASHINGTON verified (201) 233-9590 as his current number and 2016 S104th Street, Burien, Washington (**Target Premises #3**) as his current billing address.

1        56. On December 19, 2023, DEA Atlanta obtained a geolocation search  
2 warrant for (201) 233-9590, the cellular device known to be used by WASHINGTON.

3        57. A review of overnight and daytime activity for both historical location data  
4 and live geolocation data shows WASHINGTON's cellular facilities consistently  
5 connecting to the cell sites in the area of **Target Premises #3**. DEA agents also observed  
6 via a static surveillance platform (pole camera) WASHINGTON at **Target Premises #3**,  
7 as recently as January 10, 2024.

8        58. The review of the geolocation data also shows that WASHINGTON sleeps  
9 at **Target Premises #3** and remains there throughout the night hours on several  
10 occasions. Based on the surveillance, the geolocation data, and my training and  
11 experience, I believe that **Target Premises #3** is WASHINGTON's primary address.

12        59. Occasionally, WASHINGTON will spend the night at 802 S 31st St,  
13 Renton, Washington (**Target Premises #4**), a residence believed to be his girlfriend's  
14 residence. and that he occasionally spends some nights at his girlfriend's residence;  
15 **Target Premises #4**.

16        **Identification of 802 S 31st St, Renton, Washington "Target Premise #4"**

17        60. Upon reviewing both historical location data and live geolocation data for  
18 WASHINGTON's cellular facilities agents identified WASHINGTON consistently  
19 connecting to the cell sites in the area of **Target Premise #4**. WASHINGTON has and  
20 continues to spend a considerable amount of time at **Target Premise #4** and would  
21 occasionally sleep at **Target Premise #4** and remain at **Target Premise #4** throughout  
22 the night and early morning hours.

23        61. A search of law enforcement data bases as well as an open source search  
24 identified that **Target Premise #4** is associated with Dominique Lee. Agents identified a  
25 phone number associated with Lee and that phone number is in contact with  
26 WASHINGTON and is one of his top callers. A search of social media accounts  
27 associated with Lee, led agents to identify a Facebook account believed to belong to Lee.

1 A review of the Facebook account, agents located two photographs that were posted, one  
2 dated June 5, 2023, and the other on April 6, 2022, both of which depict WASHINGTON  
3 and a small child together. Based on the photographs and review of the Facebook  
4 account agents believe that WASHINGTON is the father of the small child and Lee is the  
5 mother. Agents believe that WASHINGTON is splitting time between **Target Premise**  
6 **#3** and **Target Premise #4** due to WASHINGTON's child living at **Target Premise #4**.

7 62. On January 9, 2024, agents observed WASHINGTON exit **Target Premise**  
8 **#4** and get into a Buick Enclave bearing WA tag A6873816, that was parked in the  
9 driveway of **Target Premise #4**. The Buick Enclave bearing WA tag A6873816 is  
10 registered to Dominique LEE. WASHINGTON was then observed pulling out of the  
11 driveway and departing **Target Premise #4**. Agents were able to confirm that the live  
12 geolocation data from WASHINGTON's cellular devices was traveling in tandem with  
13 WASHINGTON as he left **Target Premise #4**. Agents monitored the data which showed  
14 WASHINGTON travel to an industrial complex with several business. Agents were able  
15 to follow the geolocation data and locate the Enclave in the parking lot but the vehicle  
16 was unoccupied. Agents maintained surveillance on the Enclave and eventually observed  
17 WASHINGTON get back into the Enclave. Agents maintained constant surveillance on  
18 the Enclave as it left the parking lot and drove directly to **Target Premise #3**. Again, the  
19 geolocation data for WASHINGTON's phone traveled in tandem with WASHINGTON  
20 driving to **Target Premise #3**. Agents observed via a pole camera at **Target Premise #3**,  
21 WASHINGTON walk up the steps and enter into **Target Premise #3**.

22 63. Based on a review of the historical location data and live geolocation data  
23 for WASHINGTON's phone, the phone does not remain constantly on. It appears the  
24 phone is turned off then turned on periodically. Based on my training and experience this  
25 behavior is consistent with a person who has multiple phones as well as a person that is  
26 trying to avoid being tracked by law enforcement. Often a person who is trying to avoid  
27

1 detection from law enforcement, would turn their phone off so law enforcement cannot  
2 track them via their cell phone.

3 **Identification of 1838 E 34th Street, Tacoma, WA “Target Premise #5”**

4 64. During the investigation, agents identified a T-Mobile cellular device  
5 assigned call number (404) 604-1138, subscribed in the name of RUSSELL BANETT at  
6 1838 E 34TH ST TACOMA WA 98404-4803 (**Target Premise #5**), which is believed to  
7 be used by DTO member Maurice LYNCH.

8 65. After his arrest on July 18, 2022, M. LYNCH’s cellular telephone was  
9 seized as evidence. That telephone was subscribed in the name “RUSSELL BANETT,”  
10 and is still in the possession of law enforcement. M. LYNCH was released on bond from  
11 the Fulton County (GA) Jail on July 20, 2022. On July 23, 2022, the cellular device  
12 assigned call number (404) 604-1138 was activated, and subscribed under the name  
13 “RUSSELL BANETT” at 1838 E 34TH ST TACOMA WA 98404-4803 (**Target**  
14 **Premise #5**).

15 66. On December 29, 2023, DEA agents observed via a static surveillance  
16 platform (pole camera) Ramondo LYNCH at **Target Premise #5**. Based on geolocation  
17 data from R. LYNCH’s cellular device, it revealed that R. LYNCH stayed at **Target**  
18 **Premise #5** overnight for several days. DEA Seattle agents also observed M. LYNCH at  
19 **Target Premise #5**.

20 67. On January 3, 2024, DEA Atlanta obtained a geolocation search warrant for  
21 the cellular device that is known to be used by M. LYNCH. A review of overnight  
22 activity for both historical location data and live geolocation data showed M. LYNCH’s  
23 phone connecting to the cell sites near **Target Premise #5** almost every night and into  
24 the early morning hours.

25 68. During the investigation agents identified an Instagram Account with the  
26 name @executiveprints, which is associated with and belongs to Ramondo LYNCH  
27 (brother of M. LYNCH). On or about February 16, 2023, DEA located several



1 | photographs and videos posted on Instagram by R. LYNCH via @executiveprints, which  
2 | depict R. LYNCH walking in the back yard of a residence. In the video you can see the  
3 | back of the residence and the surrounding area. The video is also tagged with the location  
4 | as Seattle, WA. Additional videos and photographs depicted several French bulldogs on  
5 | the property and large unique black cages that contained more dogs.

6 |         69. By comparing the photographs and videos posted by R. LYNCH, to the  
7 | back yard of **Target Premise #5** agents were able to determine that the photographs and  
8 | videos were taken in the back yard of **Target Premise #5**. The large black dog cages and  
9 | the dogs themselves in the photographs and videos appear to be the same type seen  
10 | during the search warrant execution at the DTO stash house on July 18, 2022, in  
11 | Fairburn, Georgia.

12 |         70. Based on reviewing the pattern of life via the geolocation data received as  
13 | of January 9, 2024, agents believe that M. LYNCH will be present inside of **Target**  
14 | **Premise #5**, when agents anticipate executing the Search warrants.

15 |         71. In virtually every DTO stash house where agents have executed search  
16 | warrants, documents and cell phones have been seized, almost all of which contained  
17 | evidence of the DTO's operations. Based on my training, experience, and knowledge of  
18 | the investigation to date, I believe that there is evidence of the DTO's cocaine trafficking  
19 | operations, and communications and coordination between the members in furtherance of  
20 | the DTO contained within the **Target Premises**. I believe a search of the **Target**  
21 | **Premises** will yield documentary evidence of the drug trafficking activities of this DTO,  
22 | including but not limited to: drug and money ledgers, bank account information,  
23 | telephone numbers, telephone books, address books, credit card and hotel receipts, plane  
24 | and bus tickets and receipts, car rental receipts, passports, accounts and records in  
25 | fictitious names, false identification, money orders, cashier's checks relating to cash  
26 | transactions, and records indicating the existence of storage facilities and other locations  
27 | utilized by the DTO known or yet unknown. I believe searching the **Target Premises**

1 will lead to the identification and location of additional electronic devices that are used  
2 by the Target Subjects. Electronic devices used by DTO members will contain valuable  
3 evidence associated with the DTO's cocaine trafficking operations. Additionally, I  
4 believe a search of the **Target Premises** will reveal aftermarket hidden compartments in  
5 vehicles and secret rooms contained within the **Target Premises** that may contain  
6 additional evidence of the DTO's cocaine trafficking conspiracy.

7 72. Searching the **Target Premises** for those items as would most likely yield  
8 evidence to prosecute the case in chief under this current indictment.

9 **KNOWLEDGE BASED ON TRAINING AND EXPERIENCE**

10 73. During my employment with DEA, I have been active in investigations  
11 involving narcotics trafficking and distribution and money laundering. I have received  
12 training on the subject of narcotics trafficking and have been personally involved in  
13 investigations concerning the possession, manufacture, distribution, and importation of  
14 controlled substances, as well as methods used to finance drug transactions and launder  
15 drug proceeds. Further, I have and consulted with more senior agents that also have  
16 participated in many wiretap investigations that resulted in a number of arrests and  
17 seizures concerning drug trafficking and money laundering. During the course of these  
18 investigations, it was apparent that drug traffickers were using telephones in furtherance  
19 of their illegal activities. In addition, I have also analyzed telephone toll records and  
20 other records and debriefed informants regarding the use of telephones.'

21 74. Based on my training and experience, and based upon interviews I have  
22 conducted with defendants, witnesses, and informants, as well as others with knowledge  
23 of the importation, distribution, and transportation of controlled substances and of the  
24 laundering and concealing of proceeds derived from drug trafficking, I am familiar with  
25 the ways in which drug traffickers conduct their business. For example, this includes, but  
26 is not limited to, the methods of importing, packaging, transferring and distributing  
27 narcotics, the use of electronic means and cellular telephones for calls and electronic



1 communications including, but not limited to, email and text messaging, the use of  
2 numerical codes, code words and other methods of avoiding detection by law  
3 enforcement.

4 75. I am also familiar with the types and amounts of profits made by narcotics  
5 dealers and the methods, language and terms that are used to disguise the source and  
6 nature of the profits from their illegal narcotics dealing. Additionally, I have learned  
7 about the ways that drug traffickers conceal, convert, transmit, and transport their drug  
8 proceeds, including but not limited to, the use of runners/couriers to transport currency  
9 and proceeds, the use of third parties to purchase or hold title to assets, and the use of off  
10 shore accounts. Finally, I have written and/or executed search, seizure, and arrest  
11 warrants pertaining to the seizure of all types of criminal evidence, including illegal  
12 drugs, drug paraphernalia, drug proceeds, drug records, and evidence of other types of  
13 crimes.

14 76. Based on my training, experience, and discussions with senior agents, I  
15 know that drug trafficking is often furthered by utilizing multiple cellular phones,  
16 multiple insulated contacts, pre-paid cellular phones, and phones designated to be used  
17 only for certain purposes or individuals, which is also known as compartmentalization. I  
18 also know that narcotics traffickers often attempt to thwart law enforcement efforts by  
19 frequently changing and fictitiously registering vehicles, telephones, and utility services  
20 in order to conceal their true identity. I also know it is common for narcotics traffickers to  
21 conduct counter surveillance as well as perform "heat checks" to avoid law enforcement  
22 and aid in identifying if law enforcement is following the drug traffickers. All of these  
23 steps are designed to avoid detection by law enforcement and possible prosecution.

24 77. Based on my training, experience, discussions with other agents and other  
25 law enforcement officers, I am aware that individuals who participate in crimes often use  
26 cell phones and online tools to facilitate and plan their criminal activity to include  
27 avoiding detection by law enforcement. Specifically, I am aware that individuals

1 commonly use cell phones before, during, and after the commission of crimes to  
2 coordinate the crimes.

3 78. I know, based upon my training, experience, and discussions with senior  
4 agents that narcotics trafficking and money laundering organizations routinely utilize a  
5 number of other operational techniques designed to achieve two goals: first, the  
6 successful facilitation of the organization's illegal activities, including the transportation  
7 and distribution of controlled substances and the subsequent collection of the proceeds of  
8 that illegal activity; and second, minimizing the exposure of organization members,  
9 particularly those operating in management roles, from investigation and prosecution by  
10 law enforcement.

11 79. I have participated in this investigation and I am thoroughly familiar with  
12 the information contained herein either through personal investigation or through  
13 discussions with agents from other law enforcement agencies who have interviewed the  
14 individuals or who have personally obtained information that they have reported to me.  
15 Based on training, experience, and participation in narcotic and drug-related  
16 investigations, I know that:

17 a. Individuals who deal in illegal controlled substances  
18 commonly maintain books, records, receipts, notes, ledgers, bank records,  
19 money orders, and other papers relating to the importation, manufacture,  
20 transportation, ordering, sale, and distribution of illegal controlled  
21 substances. These items are typically maintained where the dealers in  
22 illegal controlled substances have ready access to them, such as in secured  
23 locations within their residence, the residences of friends, family members,  
24 significant others, and associates, or in the places of operation of the drug  
25 distribution activity, such as a stash house or safe house. Moreover, it is  
26 common that traffickers maintain such records on computers, cellular  
27

1       telephones, personal tablets, laptop computers, and other personal  
2       electronic devices.

3               b.       Individuals who deal in illegal controlled substances routinely  
4       conceal in their residences or the residences of friends, family members,  
5       significant others, and associates, or in the places of operation of the drug  
6       distribution activity, such as a stash house or safe house, large quantities of  
7       currency, financial instruments, precious metals, jewelry, and other items of  
8       value that are typically the proceeds of illegal controlled substance  
9       transactions.

10              c.       It is common for individuals who deal in the sale and  
11       distribution of illegal controlled substance, money laundering, and other  
12       criminal activity to utilize alternative currency such as cryptocurrency or  
13       digital currency, in an attempt to avoid detection from law enforcement. It  
14       is also common for these individuals to utilize storage devices commonly  
15       referred to cold storage devices to store large amounts of digital currency. It  
16       is also known that these individuals often maintain a key that is used to  
17       secure and control access to digital assets, such as cryptocurrency and other  
18       blockchain- based assets. It is also known that these individuals often  
19       maintain a seed phrases, a sequence of random words that stores the data  
20       required to access or recover cryptocurrency on blockchains or crypto  
21       wallets.

22              d.       It is common for individuals who deal in the sale and  
23       distribution of illegal controlled substances to secret contraband related to  
24       the activity, such as scales, razors, packaging materials, cutting agents,  
25       cooking utensils, microwave ovens, pots, dishes, and other containers, at  
26       their residences, or the residences of friends, family members, significant  
27

1 others, or associates, or in the places of operation of the drug distribution  
2 activity, such as a stash house or safe house.

3 e. Individuals who deal in the sale and distribution of controlled  
4 substances commonly maintain addresses and telephone number books or  
5 papers, which reflect names, addresses or telephone numbers for their  
6 associates in their illegal organization. These individuals often utilize  
7 cellular telephones, pagers, and telephone systems to maintain contact with  
8 their associates in their illegal businesses. These telephone records, bills,  
9 and pager numbers are often found in their place of residence, or the  
10 residence of friends, family members, significant others, or associates, or in  
11 the places of operation of the drug distribution activity, such as a stash  
12 house or safe house.

13 f. Individuals who deal in illegal controlled substances often  
14 take photos of themselves, their associates, their property, and illegal  
15 contraband. These photos are usually maintained in their place of  
16 residence, or the residences of friends, family members, significant others,  
17 or associates, or in the places of operation of the drug distribution activity,  
18 such as a stash house or safe house.

19 g. Persons who traffic controlled substances commonly maintain  
20 documents, letters, and records relating to illegal activity for long periods  
21 of time. This documentary evidence is usually secreted in their residence,  
22 or the residences of friends, family, significant others, members or  
23 associates, or in the places of operation of the drug distribution activity,  
24 such as a stash house or safe house. This documentary evidence includes,  
25 but is not limited to, telephone numbers, telephone books, address books,  
26 credit card and hotel receipts, plane and bus tickets and receipts, car rental  
27 receipts, passports, accounts and records in fictitious names, false

1 identification, money orders, cashier's checks relating to cash transactions,  
2 and records indicating the existence of storage facilities used in narcotics  
3 trafficking. Indicia of occupancy, residency or ownership of the premises  
4 to be searched are often present in such premises.

5 h. Individuals involved in drug trafficking often own, possess or  
6 use weapons, including firearms, as a means to facilitate their illegal drug  
7 activities. Such weapons are most often secreted in their residence, or the  
8 residences of friends, family members, significant others, or associates, or  
9 in the places of operation of the drug distribution activity, such as a stash  
10 house or safe house.

11 i. Individuals involved in drug trafficking commonly keep in  
12 their residences, businesses, and vehicles cellular telephones, telephone  
13 paging devices, and computers that they utilize to assist them in the conduct  
14 of their illegal business. The memory and contents contained on these items  
15 may contain evidence of drug trafficking activity. Many drug traffickers use  
16 more than one cellular telephone at the same time to conduct their drug  
17 trafficking activity and attempt to "compartmentalize" their  
18 communications—limit the use of particular cellular telephones with a  
19 particular individual or individuals—in order to minimize the risk of the  
20 interception of their communications by law enforcement.

21 j. Individuals involved in drug trafficking often change their  
22 cellular telephone numbers and the physical phone handsets that they use to  
23 communicate when conducting their drug trafficking activities to minimize  
24 the risk of successful electronic interception and surveillance of their  
25 communications by law enforcement. In my experience, drug traffickers  
26 sometime keep the old physical phones with the intention of later changing  
27 the cellular telephone number associated with the physical phone in order

1 to use the phone again in the future to communicate with their drug  
2 trafficking associates. These phones and electronic storage memory for the  
3 phones—SIM cards, SD cards, and micro-SD cards—are frequently stored  
4 inside the drug traffickers' residences or businesses.

5 k. In addition to routinely communicating by various and  
6 changing cellular phones and telephone numbers through voice calls, drug  
7 traffickers commonly communicate about their drug trafficking activities  
8 through Short Messaging Service ("SMS") or Multimedia Messaging  
9 Service ("MMS") text messages, and also at times through instant  
10 messaging. These messages can remain on the physical phone for indefinite  
11 periods of time and often can be recovered through forensic search of the  
12 physical phone, even when the messages have been deleted by the user.  
13 Some of these messages include photographs or documents.

14 l. Individuals involved in drug trafficking are increasingly  
15 purchasing and using more sophisticated phones, such as Apple iPhones or  
16 Google Android system phones, that can connect to the internet over a  
17 wireless network and send and receive messages and attachments through  
18 internet-based email accounts and social networking accounts like  
19 Facebook and others. In my experience, drug traffickers are increasingly  
20 communicating with each other regarding their drug trafficking activities  
21 over the internet, including through the use of these internet-based email  
22 and private messaging media. "Smartphones" and computers are frequently  
23 kept inside the drug trafficker's residences, businesses, and vehicles.

#### 24 **SEARCH OF DIGITAL DEVICES**

25 80. The warrant I am applying for would permit law enforcement to obtain  
26 from certain individuals the display of physical biometric characteristics (such as  
27 fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to

1 search and seizure pursuant to this warrant. I seek this authority based on the following:

- 2 a. I know from my training and experience, as well as from information found  
3 in publicly available materials published by device manufacturers, that  
4 many electronic devices, particularly newer mobile devices and laptops,  
5 offer their users the ability to unlock the device through biometric features  
6 in lieu of a numeric or alphanumeric passcode or password. These  
7 biometric features include fingerprint scanners and facial recognition  
8 features. Some devices offer a combination of these biometric features, and  
9 the user of such devices can select which features they would like to utilize.
- 10 b. If a device is equipped with a fingerprint scanner, a user may enable the  
11 ability to unlock the device through his or her fingerprints. For example,  
12 Apple offers a feature called “Touch ID,” which allows a user to register up  
13 to five fingerprints that can unlock a device. Once a fingerprint is  
14 registered, a user can unlock the device by pressing the relevant finger to  
15 the device’s Touch ID sensor, which is found in the round button (often  
16 referred to as the “home” button) located at the bottom center of the front of  
17 the device. The fingerprint sensors found on devices produced by other  
18 manufacturers have different names but operate similarly to Touch ID.
- 19 c. If a device is equipped with a facial recognition feature, a user may enable  
20 the ability to unlock the device through his or her face, iris, or retina. For  
21 example, Apple offers a facial recognition feature called “Face ID.” During  
22 the Face ID registration process, the user holds the device in front of his or  
23 her face. The device’s camera then analyzes and records data based on the  
24 user’s facial characteristics. The device can then be unlocked if the camera  
25 detects a face with characteristics that match those of the registered face.  
26 Facial recognition features found on devices produced by other  
27 manufacturers have different names but operate similarly to Face ID.

- 1 d. While not as prolific on digital devices as fingerprint and facial-recognition  
2 features, both iris and retina scanning features exist for securing  
3 devices/data. The human iris, like a fingerprint, contains complex patterns  
4 that are unique and stable. Iris recognition technology uses mathematical  
5 pattern-recognition techniques to map the iris using infrared light.  
6 Similarly, retina scanning casts infrared light into a person's eye to map the  
7 unique variations of a person's retinal blood vessels. A user can register  
8 one or both eyes to be used to unlock a device with these features. To  
9 activate the feature, the user holds the device in front of his or her face  
10 while the device directs an infrared light toward the user's face and  
11 activates an infrared sensitive camera to record data from the person's eyes.  
12 The device is then unlocked if the camera detects the registered eye.
- 13 e. In my training and experience, users of electronic devices often enable the  
14 aforementioned biometric features because they are considered to be a more  
15 convenient way to unlock a device than by entering a numeric or  
16 alphanumeric passcode or password. Moreover, in some instances,  
17 biometric features are considered to be a more secure way to protect a  
18 device's contents. This is particularly true when the users of a device are  
19 engaged in criminal activities and thus have a heightened concern about  
20 securing the contents of a device.
- 21 f. As discussed in this affidavit, based on my training and experience I  
22 believe that one or more digital devices will be found during the search.  
23 The passcode or password that would unlock the device(s) subject to search  
24 under this warrant is not known to law enforcement. Thus, law enforcement  
25 personnel may not otherwise be able to access the data contained within the  
26 device(s), making the use of biometric features necessary to the execution  
27 of the search authorized by this warrant.



- 1 g. I also know from my training and experience, as well as from information  
2 found in publicly available materials including those published by device  
3 manufacturers, that biometric features will not unlock a device in some  
4 circumstances even if such features are enabled. This can occur when a  
5 device has been restarted, inactive, or has not been unlocked for a certain  
6 period of time. For example, Apple devices cannot be unlocked using  
7 Touch ID when (1) more than 48 hours has elapsed since the device was  
8 last unlocked or (2) when the device has not been unlocked using a  
9 fingerprint for 4 hours *and* the passcode or password has not been entered  
10 in the last 156 hours. Biometric features from other brands carry similar  
11 restrictions. Thus, in the event law enforcement personnel encounter a  
12 locked device equipped with biometric features, the opportunity to unlock  
13 the device through a biometric feature may exist for only a short time.
- 14 h. In my training and experience, the person who is in possession of a device  
15 or has the device among his or her belongings at the time the device is  
16 found is likely a user of the device. However, in my training and  
17 experience, that person may not be the only user of the device, and may not  
18 be the only individual whose physical characteristics are among those that  
19 will unlock the device via biometric features. Furthermore, while physical  
20 proximity is an important factor in determining who is the user of a device,  
21 it is only one among many other factors that may exist.
- 22 i. Due to the foregoing, I request that if law enforcement personnel encounter  
23 a device that is subject to search and seizure pursuant to this warrant and  
24 may be unlocked using one of the aforementioned biometric features, and if  
25 law enforcement reasonably suspects Mario James EARL, Elisa  
26 JOHNSON, Maurice LYNCH, and/or Turomne WASHINGTON is a user  
27 of the device, then – for the purpose of attempting to unlock the device in

1 order to search the contents as authorized by this warrant – law  
2 enforcement personnel shall be authorized to:(1) press or swipe the fingers  
3 (including thumbs) of Mario James EARL, Elisa JOHNSON, Maurice  
4 LYNCH, and/or Turomne WASHINGTON to the fingerprint scanner of the  
5 device; and/or (2) hold the device in front of the face and open eyes of  
6 those same individuals and activate the facial, iris, or retina recognition  
7 feature.

8 j. In pressing or swiping an individual's thumb or finger onto a device and in  
9 holding a device in front of an individual's face and open eyes, law  
10 enforcement may not use excessive force, as defined in *Graham v. Connor*,  
11 490 U.S. 386 (1989); specifically, law enforcement may use no more than  
12 objectively reasonable force in light of the facts and circumstances  
13 confronting them.

14 81. As outlined above, in addition to cellular telephones, there is probable  
15 cause to believe that members of the conspiracy use computers (desktop or laptops) to  
16 facilitate their criminal activity. Members of the conspiracy are believed to email among  
17 themselves instructions and information about the conspiracy and to coordinate their  
18 activities via that means of communication. There is also probable cause to believe that  
19 members of the conspiracy use computers to launder their illegal proceeds, for example  
20 by using the computer to facilitate investments in real property or other assets.

21 82. I know, based on my training, experience, and knowledge of this  
22 investigation that much of the evidence of these crimes can be stored as data on digital  
23 devices like computers and cellular telephones. Thus, the warrant applied for would  
24 authorize the seizure of digital devices or other electronic storage media or, potentially,  
25 the copying of electronically stored information from digital devices or other electronic  
26 storage media, all under Rule 41(e)(2)(B).

1       83. Based upon my review of the evidence gathered in this investigation, my  
2 review of data and records, information received from other agents and computer  
3 forensics examiners, and my training and experience, I submit that if a digital device or  
4 other electronic storage media is found at the **TARGET PREMISES**, there is probable  
5 cause to believe that evidence of the crimes of discussed above will be stored on those  
6 digital devices or other electronic storage media, and that those digital devices are  
7 instrumentalities of said crime.

8       84. There is, therefore, probable cause to believe that evidence of the crimes of  
9 described above and in Attachment B exists and will be found on digital device or other  
10 electronic storage media at the **TARGET PREMISES**, for at least the following reasons:

- 11       a. Based on my knowledge, training, and experience, I know that computer  
12 files or remnants of such files can be preserved (and consequently also then  
13 recovered) for months or even years after they have been downloaded onto  
14 a storage medium, deleted, or accessed or viewed via the Internet.  
15 Electronic files downloaded to a digital device or other electronic storage  
16 medium can be stored for years at little or no cost. Even when files have  
17 been deleted, they can be recovered months or years later using forensic  
18 tools. This is so because when a person “deletes” a file on a digital device  
19 or other electronic storage media, the data contained in the file does not  
20 actually disappear; rather, that data remains on the storage medium until it  
21 is overwritten by new data.
- 22       b. Therefore, deleted files, or remnants of deleted files, may reside in free  
23 space or slack space—that is, in space on the digital device or other  
24 electronic storage medium that is not currently being used by an active  
25 file—for long periods of time before they are overwritten. In addition, a  
26 computer’s operating system may also keep a record of deleted data in a  
27 “swap” or “recovery” file.
- 28       c. Wholly apart from user-generated files, computer storage media—in  
29 particular, computers’ internal hard drives—contain electronic evidence of  
30 how a computer has been used, what it has been used for, and who has used  
31 it. To give a few examples, this forensic evidence can take the form of  
32 operating system configurations, artifacts from operating system or  
33 application operation; file system data structures, and virtual memory  
34 “swap” or paging files. Computer users typically do not erase or delete this  
35 evidence, because special software is typically required for that task.  
36 However, it is technically possible to delete this information.

1 d. Similarly, files that have been viewed via the Internet are sometimes  
2 automatically downloaded into a temporary Internet directory or “cache.”

3 85. *Forensic evidence.* As further described in Attachment B, this application  
4 seeks permission to locate not only computer files that might serve as direct evidence of  
5 the crimes described on the warrant, but also for forensic electronic evidence that  
6 establishes how digital devices or other electronic storage media were used, the purpose  
7 of their use, who used them, and when. There is probable cause to believe that this  
8 forensic electronic evidence will be on any digital devices or other electronic storage  
9 media located at the **TARGET PREMISES** because:

10 a. Stored data can provide evidence of a file that was once on the digital  
11 device or other electronic storage media but has since been deleted or edited, or  
12 of a deleted portion of a file (such as a paragraph that has been deleted from a  
13 word processing file). Virtual memory paging systems can leave traces of  
14 information on the digital device or other electronic storage media that show  
15 what tasks and processes were recently active. Web browsers, e-mail  
16 programs, and chat programs store configuration information that can reveal  
17 information such as online nicknames and passwords. Operating systems can  
18 record additional information, such as the history of connections to other  
19 computers, the attachment of peripherals, the attachment of USB flash storage  
20 devices or other external storage media, and the times the digital device or  
21 other electronic storage media was in use. Computer file systems can record  
22 information about the dates files were created and the sequence in which they  
23 were created.

24 b. As explained herein, information stored within a computer and other  
25 electronic storage media may provide crucial evidence of the “who, what, why,  
26 when, where, and how” of the criminal conduct under investigation, thus  
27 enabling the United States to establish and prove each element or alternatively,  
to exclude the innocent from further suspicion. In my training and experience,  
information stored within a computer or storage media (e.g., registry  
information, communications, images and movies, transactional information,  
records of session times and durations, internet history, and anti-virus,  
spyware, and malware detection programs) can indicate who has used or  
controlled the computer or storage media. This “user attribution” evidence is  
analogous to the search for “indicia of occupancy” while executing a search  
warrant at a residence. The existence or absence of anti-virus, spyware, and  
malware detection programs may indicate whether the computer was remotely  
accessed, thus inculcating or exculpating the computer owner and/or others

1 with direct physical access to the computer. Further, computer and storage  
2 media activity can indicate how and when the computer or storage media was  
3 accessed or used. For example, as described herein, computers typically  
4 contain information that log: computer user account session times and  
5 durations, computer activity associated with user accounts, electronic storage  
6 media that connected with the computer, and the IP addresses through which  
7 the computer accessed networks and the internet. Such information allows  
8 investigators to understand the chronological context of computer or electronic  
9 storage media access, use, and events relating to the crime under  
10 investigation.<sup>10</sup> Additionally, some information stored within a computer or  
11 electronic storage media may provide crucial evidence relating to the physical  
12 location of other evidence and the suspect. For example, images stored on a  
13 computer may both show a particular location and have geolocation  
14 information incorporated into its file data. Such file data typically also  
15 contains information indicating when the file or image was created. The  
16 existence of such image files, along with external device connection logs, may  
17 also indicate the presence of additional electronic storage media (e.g., a digital  
18 camera or cellular phone with an incorporated camera). The geographic and  
19 timeline information described herein may either inculcate or exculpate the  
20 computer user. Last, information stored within a computer may provide  
21 relevant insight into the computer user's state of mind as it relates to the  
22 offense under investigation. For example, information within the computer  
23 may indicate the owner's motive and intent to commit a crime (e.g., internet  
24 searches indicating criminal planning), or consciousness of guilt (e.g., running  
25 a "wiping" program to destroy evidence on the computer or password  
26 protecting/encrypting such evidence in an effort to conceal it from law  
27 enforcement).

c. A person with appropriate familiarity with how a digital device or other  
electronic storage media works can, after examining this forensic evidence in  
its proper context, draw conclusions about how the digital device or other  
electronic storage media were used, the purpose of their use, who used them,  
and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or  
other forms of forensic evidence on a digital device or other electronic storage  
media that are necessary to draw an accurate conclusion is a dynamic process.  
While it is possible to specify in advance the records to be sought, digital

---

<sup>10</sup> For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

1 evidence is not always data that can be merely reviewed by a review team and  
2 passed along to investigators. Whether data stored on a computer is evidence  
3 may depend on other information stored on the computer and the application of  
4 knowledge about how a computer behaves. Therefore, contextual information  
5 necessary to understand other evidence also falls within the scope of the  
6 warrant.

7 e. Further, in finding evidence of how a digital device or other electronic  
8 storage media was used, the purpose of its use, who used it, and when,  
9 sometimes it is necessary to establish that a particular thing is not present. For  
10 example, the presence or absence of counter-forensic programs or anti-virus  
11 programs (and associated data) may be relevant to establishing the user's  
12 intent.

13 86. I know based on my training and experience that digital information can be  
14 very fragile and easily destroyed. Digital information can also be easily encrypted or  
15 obfuscated such that review of the evidence would be extremely difficult, and in some  
16 cases impossible. As outlined above, there is probable cause to believe that M. EARL  
17 uses encryption on the computer systems he utilizes to engage in his crimes. If an  
18 encrypted computer is either powered off or if the user has not entered the encryption  
19 password and logged onto the computer, it is likely that any information contained on the  
20 computer will be impossible to decipher. If the computer is powered on, however, and  
21 the user is already logged onto the computer, there is a much greater chance that the  
22 digital information can be extracted from the computer. This is because when the  
23 computer is on and in use, the password has already been entered and the data on the  
24 computer is accessible. However, giving the owner of the computer time to activate a  
25 digital security measure, pull the power cord from the computer, or even log off of the  
26 computer could result in a loss of digital information that could otherwise have been  
27 extracted from the computer.

87. *Necessity of seizing or copying entire computers or storage media.* In most  
cases, a thorough search of premises for information that might be stored on digital  
devices or other electronic storage media often requires the seizure of the physical items  
and later off-site review consistent with the warrant. In lieu of removing all of these



1 items from the premises, it is sometimes possible to make an image copy of the data on  
2 the digital devices or other electronic storage media, onsite. Generally speaking, imaging  
3 is the taking of a complete electronic picture of the device's data, including all hidden  
4 sectors and deleted files. Either seizure or imaging is often necessary to ensure the  
5 accuracy and completeness of data recorded on the item, and to prevent the loss of the  
6 data either from accidental or intentional destruction. This is true because of the  
7 following:

8       a. *The time required for an examination.* As noted above, not all evidence  
9 takes the form of documents and files that can be easily viewed on site.  
10 Analyzing evidence of how a computer has been used, what it has been used  
11 for, and who has used it requires considerable time, and taking that much time  
12 on premises could be unreasonable. As explained above, because the warrant  
13 calls for forensic electronic evidence, it is exceedingly likely that it will be  
14 necessary to thoroughly examine the respective digital device and/or electronic  
15 storage media to obtain evidence. Computer hard drives, digital devices and  
16 electronic storage media can store a large volume of information. Reviewing  
17 that information for things described in the warrant can take weeks or months,  
18 depending on the volume of data stored, and would be impractical and invasive  
19 to attempt on-site.

20       b. *Technical requirements.* Digital devices or other electronic storage media  
21 can be configured in several different ways, featuring a variety of different  
22 operating systems, application software, and configurations. Therefore,  
23 searching them sometimes requires tools or knowledge that might not be  
24 present on the search site. The vast array of computer hardware and software  
25 available makes it difficult to know before a search what tools or knowledge  
26 will be required to analyze the system and its data on the premises. However,  
27 taking the items off-site and reviewing them in a controlled environment will  
allow examination with the proper tools and knowledge.

28       c. *Variety of forms of electronic media.* Records sought under this warrant  
29 could be stored in a variety of electronic storage media formats and on a  
30 variety of digital devices that may require off-site reviewing with specialized  
31 forensic tools.

32       88. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal  
33 Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging,  
34 or otherwise copying digital devices or other electronic storage media that reasonably



1 appear capable of containing some or all of the data or items that fall within the scope of  
 2 Attachment B to this Affidavit, and will specifically authorize a later review of the media  
 3 or information consistent with the warrant.

4 89. Consistent with the above, I hereby request the Court's permission to seize  
 5 and/or obtain a forensic image of digital devices or other electronic storage media that  
 6 reasonably appear capable of containing data or items that fall within the scope of  
 7 Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or  
 8 other electronic storage media and/or forensic images, using the following procedures:

9 **1. Processing the Search Sites and Securing the Data.**

10 a. Upon securing the physical search site, the search team will conduct an  
 11 initial review of any digital devices or other electronic storage media located at  
 12 the subject premises described in Attachment A that are capable of containing  
 13 data or items that fall within the scope of Attachment B to this Affidavit, to  
 14 determine if it is possible to secure the data contained on these devices onsite  
 15 in a reasonable amount of time and without jeopardizing the ability to  
 16 accurately preserve the data.

17 b. In order to examine the electronically stored information ("ESI") in a  
 18 forensically sound manner, law enforcement personnel with appropriate  
 19 expertise will attempt to produce a complete forensic image, if possible and  
 20 appropriate, of any digital device or other electronic storage media that is  
 21 capable of containing data or items that fall within the scope of Attachment B  
 22 to this Affidavit.<sup>1</sup>

23 c. A forensic image may be created of either a physical drive or a logical  
 24 drive. A physical drive is the actual physical hard drive that may be found in a  
 25 typical computer. When law enforcement creates a forensic image of a  
 26

---

27 <sup>1</sup> The purpose of using specially trained computer forensic examiners to conduct the  
 imaging of digital devices or other electronic storage media is to ensure the integrity of  
 the evidence and to follow proper, forensically sound, scientific procedures. When the  
 investigative agent is a trained computer forensic examiner, it is not always necessary to  
 separate these duties. Computer forensic examiners often work closely with investigative  
 personnel to assist investigators in their search for digital evidence. Computer forensic  
 examiners are needed because they generally have technological expertise that  
 investigative agents do not possess. Computer forensic examiners, however, often lack  
 the factual and investigative expertise that an investigative agent may possess on any  
 given case. Therefore, it is often important that computer forensic examiners and  
 investigative personnel work closely together.

1 physical drive, the image will contain every bit and byte on the physical drive.  
2 A logical drive, also known as a partition, is a dedicated area on a physical  
3 drive that may have a drive letter assigned (for example the c: and d: drives on  
4 a computer that actually contains only one physical hard drive). Therefore,  
5 creating an image of a logical drive does not include every bit and byte on the  
6 physical drive. Law enforcement will only create an image of physical or  
7 logical drives physically present on or within the subject device. Creating an  
8 image of the devices located at the search locations described in Attachment A  
9 will not result in access to any data physically located elsewhere. However,  
10 digital devices or other electronic storage media at the search locations  
11 described in Attachment A that have previously connected to devices at other  
12 locations may contain data from those other locations.

13  
14 d. If based on their training and experience, and the resources available to  
15 them at the search site, the search team determines it is not practical to make an  
16 on-site image within a reasonable amount of time and without jeopardizing the  
17 ability to accurately preserve the data, then the digital devices or other  
18 electronic storage media will be seized and transported to an appropriate law  
19 enforcement laboratory to be forensically imaged and reviewed.

## 2. Searching the Forensic Images.

15 a. Searching the forensic images for the items described in Attachment B may  
16 require a range of data analysis techniques. In some cases, it is possible for  
17 agents and analysts to conduct carefully targeted searches that can locate  
18 evidence without requiring a time-consuming manual search through unrelated  
19 materials that may be commingled with criminal evidence. In other cases,  
20 however, such techniques may not yield the evidence described in the warrant,  
21 and law enforcement may need to conduct more extensive searches to locate  
22 evidence that falls within the scope of the warrant. The search techniques that  
23 will be used will be only those methodologies, techniques and protocols as  
24 may reasonably be expected to find, identify, segregate and/or duplicate the  
25 items authorized to be seized pursuant to Attachment B to this affidavit. Those  
26 techniques, however, may necessarily expose many or all parts of a hard drive  
27 to human inspection in order to determine whether it contains evidence  
described by the warrant.

### **REQUEST FOR “ALL HOURS” EXECUTION**

25 90. As outlined in paragraph 28 above, surveillance and phone tracking data  
26 show that EARL and JOHNSON frequently leave one of the **Target Premises** before 6  
27 a.m. together, likely to go to the gym. As also outlined above, both of these individuals

1 have active federal arrest warrants issued by the U.S. District Court in Atlanta. That  
2 means it may be necessary to execute the search warrant at their location outside of  
3 normal daylight hours. In addition, if EARL and JOHNSON are contacted before 6 a.m.,  
4 they may have an opportunity to alert the other targets of this investigation (who also  
5 have active arrest warrants).

6 91. Accordingly, I respectfully request that the warrants to be issued allow  
7 investigators to execute said warrants at any time of the day or night, as authorized by  
8 Title 21, United States Code, Section 879.

9 **CONCLUSION**

10 92. For the foregoing reasons, I respectfully submit there is probable cause to  
11 search the **Target Premises**, more particularly described in Attachment A hereto, for the  
12 evidence described in Attachment B hereto.

13 

14 \_\_\_\_\_  
15 Evan Leyva, Affiant  
16 Special Agent, Drug Enforcement Administration

17 The above-named agent provided a sworn statement to the truth of the foregoing  
18 affidavit by telephone on the 19<sup>th</sup> day of January, 2024.

19 

20 \_\_\_\_\_  
21 The Honorable Brian A. Tsuchida  
22 United States Magistrate Judge  
23  
24  
25  
26  
27